2016

Survey on remnant data research: the artefacts recovered and the implications in a cyber security conscious world

Michael James
Department of Defence, Australia

Patryk Szewczyk
School of Science, Edith Cowan University, p.szewczyk@ecu.edu.au

DOI: 10.4225/75/58a54dda54962
James, M. & Szewczyk, P. (2016). Survey on remnant data research: the artefacts recovered and the implications in a cyber security conscious world. In Valli, C. (Ed.). (2016). *The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia (pp.57-65).*

SURVEY ON REMNANT DATA RESEARCH: THE ARTEFACTS RECOVERED AND THE IMPLICATIONS IN A CYBER SECURITY CONSCIOUS WORLD

Michael James[1], Patryk Szewczyk[2]
[1]Department of Defence, Australia
[2]School of Science, Edith Cowan University, Perth, Australia

Abstract

The prevalence of remnant data in second hand storage media is well documented. Since 2004 there have been ten separate papers released through Edith Cowan University alone. Despite numerous government agencies providing advice on securing personal and corporate information, and news articles highlighting the need for data security, the availability of personal and confidential data on second hand storage devices is continuing, indicating a systemic laissez faire attitude to data security, even in our supposedly cyber security conscious world. The research continues, but there seems to be a lack of correlation of these studies to identify trends or common themes amongst the results. The fact that this type of research continues to be conducted highlights the deficiencies in the methods used to advertise warnings publicised by Government departments and industry experts. Major media organisations seem reluctant to broadcast these warnings, unless there is a bigger story behind the issue. This paper highlights the ongoing issues and provides insight to the factors contributing to this growing trend.

Keywords
Digital storage devices, remnant data, data recovery, privacy, data sanitisation.

INTRODUCTION

Remnant data on second hand devices has been a topic of research since 1996 (Gutmann, 1996). Over the last 10 years' numerous research projects have been completed on this very topic, but to date there has been no collective quantitative or statistical evaluation of all the results, to establish the existence of any trends or common themes. Some research has been conducted in consecutive years by the same academics, e.g. through Edith Cowan University in 2011, 2012 and 2013 (Szewczyk, Robins, & Sansurooah, 2013; Szewczyk & Sansurooah, 2011; Szewczyk & Sansurooah, 2012), and while these papers have compared the types and sizes of the memory cards purchased, there was no quantitative or qualitative analysis of the data retrieved. Another paper did make some comparisons with six years of research (Jones, Valli, Dardick, Sutherland, & Dabibi, 2009), but was limited to their own research.

Digital Storage

Large volume digital storage media is in great demand and the global market as a whole is predicted to reach $6.2 billion by the year 2022 (ReportBuyer, 2015). Advances in computer technology have lead the world to embrace the concept of big data, where more storage is required. Governments and businesses, have unique storage requirements for daily activities and are turning towards the cloud to meet these growing needs. Eventually as storage devices become obsolete and if still serviceable, will still have a monetary value.

2015 saw a decline of -9.2% in the worldwide personal and entry-level hard disk storage market (Li, 2016). This highlights a possible need for the second hand market for the selling of cheap mechanical storage to meet the needs of the home based user. A search for "used" hard disk drives on the popular online auction site eBay yielded more than 33,000 listings. Other storage media types are not immune to this. New and used thumb drives can differ in price by as much as 900% (eBay, 2016). This type of division of cost can be found across all the different types of storage from flash memory to memory cards to solid state hard drives (SSD).

Performance, larger capacities and cost are the driving factors in the growth of flash storage focused technologies (Bez & Pirovano, 2014). Flash storage technologies were predicted to increase in size during 2016 (Sliwa, 2016), this is corroborated by the announcement that Samsung will release a 32TB SSD in 2017 (Shah, 2016). However, while the cost of SSD Hard Drives remain high, the demand for traditional mechanical drives will remain (Bez & Pirovano, 2014).

Previous Research

Edith Cowan University (ECU) has hosted the Australian Digital Forensics Conference since 2006 (ECU, 2016), where numerous papers from around the world that detail research into recovered remnant data on second hand storage media have been presented. The following papers, some that where presented at the conference, and others that were not, have been analysed in this study:

- I know what you did last summer… An Investigation into Remnant Data on USB Storage Devices Sold in Australia in 2015 (Robins, Williams, & Sansurooah, 2015).
- Information Security Leakage: A Forensic Analysis of USB Storage Disks (Adam & Clarke, 2014).
- Analysis of Deletion Habits On Used USB Thumb Drives (Farden & Diesburg, 2014).
- Sellers Continue to Give Away Confidential Information on Second Hand Memory Cards Sold in Australia (Szewczyk et al., 2013a).
- The 2012 Analysis of Information Remaining on Computer Hard Disks offered for Sale on the Second Hand Market in the UAE (Jones, MArtin, & Alzaabi, 2012).
- The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia (Szewczyk & Sansurooah, 2012b).
- A 2011 investigation into remnant data on second hand memory cards sold in Australia (Szewczyk & Sansurooah, 2011).
- Data Remanence in New Zealand: 2011(Roberts & Wolfe, 2011).
- The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market (Jones, Valli, Dardick, et al., 2009).
- The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market (Jones, Valli, & Dabibi, 2009).
- The 2008 Australian study of remnant data contained on 2nd hand hard disks: the saga continues (Valli & Woodward, 2008).
- Who is Reading the Data on Your Old Computer (Mee, 2008).
- An Evaluation of Personal Health Information Remnants in Second Hand Personal Computer Disk Drives (Emam, Neri, & Jonker, 2007).
- Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks (Valli & Woodward, 2007).
- An empirical methodology derived from the analysis of information remaining on second hand hard disks (Fragkos, Mee, Xynos, & Angelopoulou, 2006).

Statistical Analysis

All of the research papers where reviewed and the data was collated. As shown in Figure 1 of the fifteen research papers, eleven have resulted in data retrieval from more than half of the items purchased, with 40% of the research resulting in data retrieval from over three quarters of the items purchased. It is interesting to note that of all the research, 11 papers recorded attempts to sanitise devices, either by delete, format or repartitioning the volumes. Of these research projects, seven (64%) recorded a sanitisation attempt rate of less than half of the items purchased, and five (45%) are below one quarter.

The quantity of sensitive personal data recovered is also seen as significant (Figure 2), when you consider this as potentially facilitating the means to engage in identity fraud. Corporate data did not fare any better and it is concerning to note that there exist companies, including those in the ICT industry that do not have effective sanitisation and disposal policies to protect their most valuable commodity – their data.

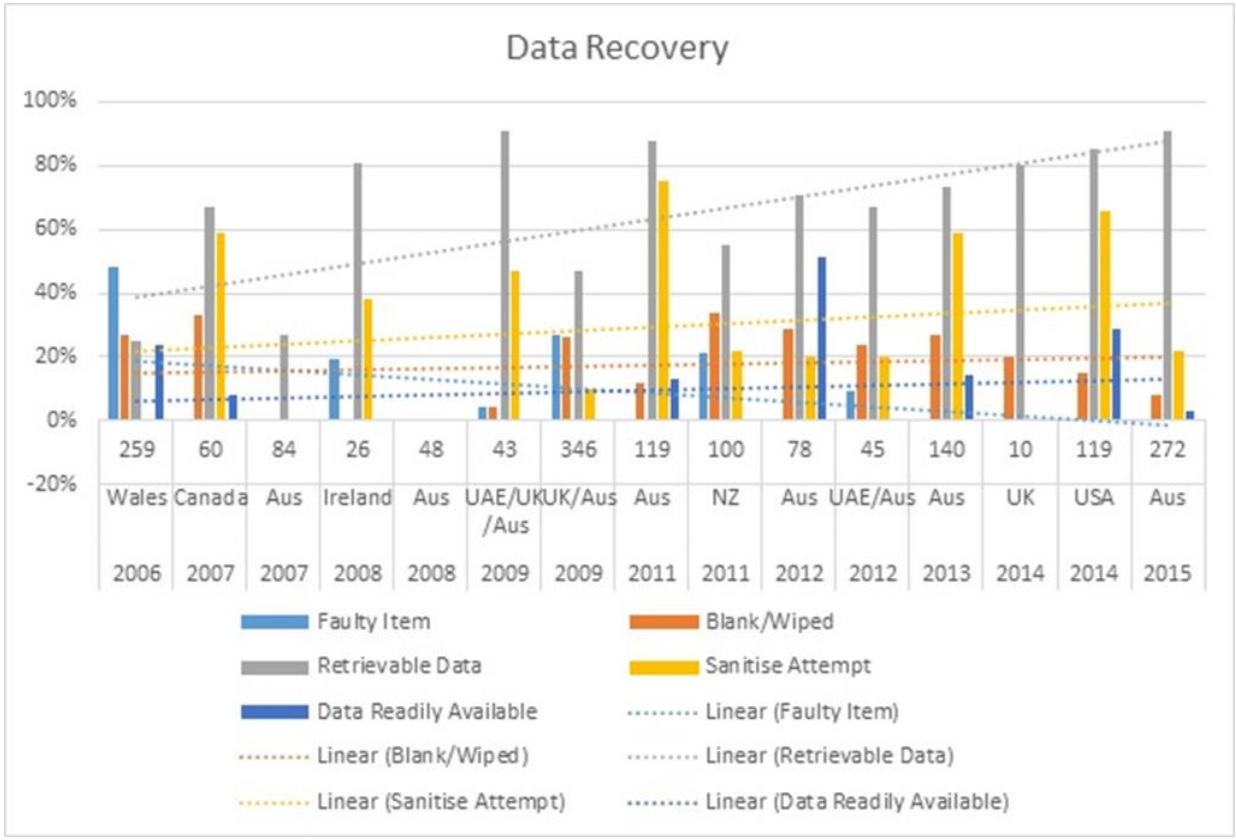

Figure 1 Statistical analysis of 15 remnant data papers with the X axis shows the year, country and number of items purchased

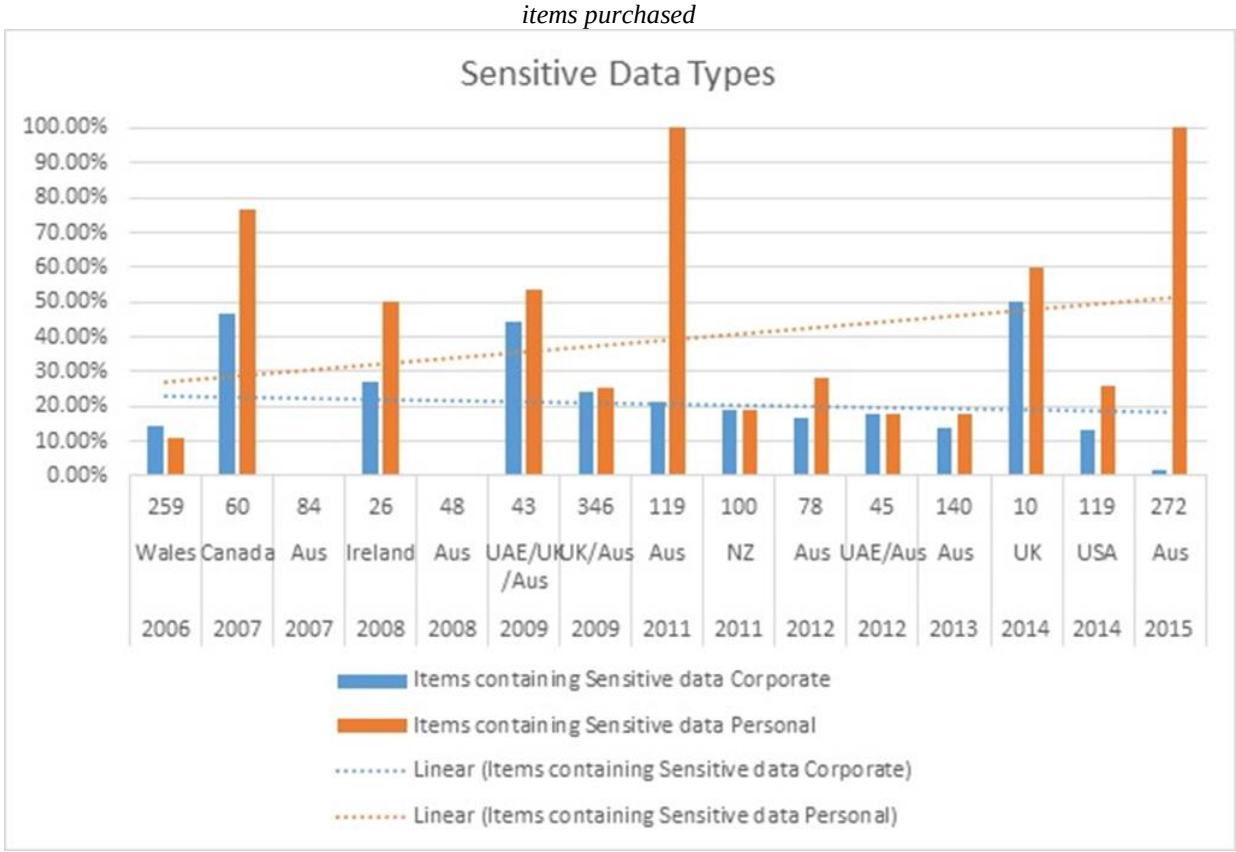

Figure 2 Statistical analysis of 15 remnant data papers with regards to sensitive data types

QUALITATIVE ANALYSIS

Common Themes

All of the research papers detailed very similar outcomes in relation to the sensitive, personal and corporate information that is more than sufficient for identity theft or industrial espionage. The majority of the research papers offered some form of reasoning behind the continuing problem from organisations lacking adequate policies, procedures and strategies that deal with the sanitisation of digital storage to the time consuming nature of developing and implementing not just the strategies and policies but the education of employees.

One common theme across the research is the premise that sellers, both corporate and private do not have an adequate understanding of how 'delete' and 'format' actually work, and have little understanding of how to correctly sanitise their digital media. In 2015 Robins, Williams and Sansurooah postulated that conflicting and misleading advice currently available on the Internet as one possible cause (Robins et al., 2015). However, the fact remains that not enough is known by the general public on how to sanitise digital storage media. Figure 2 shows a steady decline in the amount of corporate data discovered over the 10 years surveyed. This is possibly due to a greater understanding of the problems that exist, however, a number of the research papers show that there are still companies that do not take action, as stated in the 2010 Jones, Valli, Dardick, Sutherland and Dabibi paper.

Corporations spend vast amounts on the protection of data in transit and at rest, but when it comes to the storage device, there seems to be a lax approach. Considering the remnant data that potentially exists, it is strange that some sellers advertise the item for sale as coming from a corporate or government organisation. For those who deal in industrial secrets, this type of hardware would be a goldmine. Take for instance data recovered from a mining company in Australia during 2008. This project recovered supervisory control and data acquisition (SCADA) master plans and passwords, including the Administrator password, as well as photos of the mine site and employees (Valli & Woodward, 2008). Or the data recovered in Australian during the 2015 research, that included legal documents, contracts, agreements and offshore gas transportation documents marked "private and confidential" (Robins et al., 2015). Some companies have taken steps to ensure sanitisation, but are relying on third party organisations to complete the task. The risk here is the possibility that some work is substandard and leaves remnant data behind.

The datatypes that are being recovered are consistent across the entire 10 years of surveyed research. The papers detail the recovery of scanned images of passports, travel itineraries and boarding passes. PayPal and banking data, including login credentials and scanned images of credit cards have been discovered in many of the projects undertaken. Couple this with the ability to identify sellers from photographs recovered from devices and you could have the potential for disastrous consequences to occur for the seller.

Overall a common theme is that all papers report their results to be consistent with similar studies in previous years. The 2011 research completed in New Zealand found their results to be consistent with international research dating back to 2005 (Roberts & Wolfe, 2011), and a 2008 Irish paper reported results consistent with other worldwide research and showed that it was not only a problem in Ireland, but the rest of the world (Mee, 2008). Six years of research with similar results, this shows that education of the masses is either grossly ineffective or non-existent.

Trends

The statistical analysis shows that overall the amount of data retrieved has increased significantly, even though the percentage of data that is seen as 'readily available' has remained relatively static throughout the research (Figure 1). Instances of attempts to sanitise devices has steadily increased, which could be part of lack of knowledge on how 'delete' and 'format' work (this data includes successful sensitisations). An interesting trend is the sharp reduction in the faulty items being sold, which was also reported in the 2009 United Kingdom Australia paper (Jones, Valli, Dardick, et al., 2009).

The trends shown in Figure 2 is that the amount of retrievable data of a personal nature has been increasing whilst corporate data is steadily decreasing. Organisations seem to be becoming more aware of implications and risks associated with disposing of digital media. Eight research papers stated that documents relating to Government organisations were located at some point in the analysis. The latest such find was in 2015 where the construction plans for an Australian army barracks where located. This fact is surprising, when you consider the requirements of the Australian Privacy Principles imposed on all Australian Government Departments from

2013 (OAIC, 2013) and the advice published by the Australian Signals Directorate in their data sanitisation guide (ASD, 2016b).

One trend shows a degree of laziness on the part of sellers, where they are requesting the buyer to remove their data. In 2012 Australian research there were 19 instances where a note requesting the buyer to delete the contents of the device was included with the product (Szewczyk & Sansurooah, 2012). This trend continued in the 2013 Australian research, where a seller supplied a note reporting attempting to remove the data, but was unsure if it was successful and some sellers advertising on the auction listing that devices where being "sold as is" and data would not be deleted due to time constraints (Szewczyk et al., 2013a).

Each year that the research is conducted, the average storage size of the purchased second hand items has increased, this is especially true for the thumb drives and flash memory. There are two possible answers to this, one being that the cost per gigabyte is reducing and the other possibility is that users are requiring more storage space. With the increase in storage capacity, there has been an increase in the amount of retrievable data (Jones, Valli, Dardick, et al., 2009; Robins et al., 2015).

Search Engine Query – "How to delete data"

There is a significant quantity of remnant data being retrieved from second hand devices, and the Robins, Williams and Sansurooah paper mentioned the conflicting and misleading advice on the Internet. As a result an analysis of available information found on the Internet was undertaken for erasing data. The searches were conducted using Google, Bing, Yahoo and Ask, the top four English language search engines (eBiz, 2016), and the browser used was Firefox. The search term "how to erase data from a thumb drive" was used, with only the first page of search results reviewed. To ensure a clinical response, a generic new user account was created for each search engine used and no web accounts logged into.

Table 1 – Search Engine Queries for Data Erasure

	Google	Bing	Yahoo	ASK
Delete/Format	6 Windows 1 Mac	5 Windows	5 Windows	4 Windows
Wipe/Erase	1 Windows 1 Mac	1 Windows 1 Mac	2 Windows 2 Mac	3 Windows 2 Mac
Fill up and delete	1 Windows	1 Windows	1 Windows	1 Windows
Bad links		2		
Advertisements			5	10

Google
Ten results were returned. The first two results were YouTube videos on how to perform a quick format on a flash drive. The video titles were:

- "How to Erase/Delete All Data from Flash Drive Tutorial" (Rivera, 2011)
- "How to erase all content on USB Flashdrive" (Anthoct104, 2011)

Two links took the searcher to sites that detailed how to use the erase a thumb drive, one for the Apple OSX operating system and the other for Microsoft Windows. The Windows environment the tools suggested where Disk Wipe and CCleaner and MAC users where advised to open Disk Utilities and select "Erase". One forum site suggested the user fill the drive with junk, then delete the junk and repeat two more times. Of the remaining six results, the sites the user was directed to varied from forum posts to blog style instructions on how to perform a delete or format of the device. The interesting result is the descriptions used across the results, these ranged from "how to format" to "how to clear" to "how to delete".

Bing
Ten result were returned. The first two results were links to a web page and a YouTube video. The result titles where:

- "Deleting files in your flash drive or memory card using a PC" (SanDisk, 2008)
- "How to Erase/Delete All Data from Flash Drive Tutorial" (Rivera, 2011)

While there was only one result returned for Apple OSX based computers, it also detailed the use of the OSX Disk Utilities Erase function. Of the Windows based results, two where links that displayed content errors and all of the others had titles that ranged from "permanently delete files" to "How to erase all content" to "How to erase a flash drive". After result number five, Bing displayed a link tilted "Videos of how to erase data from a thumb drive". It was observed that this link title related directly to the search criteria, and when opened, a large number of videos where displayed, again with varying titles that contained the words erase, delete, wipe or format.

Yahoo

Ten results were returned, along with 5 advertisements for products, reports and tips relating to wiping data from a device. The first result was a link to a 2011 YouTube video on how to format a USB drive. The first link on how to erase a device was for an Apple OSX at result number 3 and for a PC at result number 4. Result numbers 8 – 10 also described methods for erasing data, including filling the device up with junk and deleting. Yahoo provides featured content labelled as "How to erase data from a thumb drive - Yahoo Answers results". The three items displayed had nothing to do with erasing data from a thumb drive.

ASK

Ten results – the first two results matched those of the searches completed using Google, these being:

- "How to Erase/Delete All Data from Flash Drive Tutorial" (Rivera, 2011)
- "How to erase all content on USB Flashdrive" (Anthoct104, 2011)

10 advertisements where displayed, five above and below the web results with all advertisements at the top repeated at the bottom. Two advertisements where for products that could erase storage media, however, three advertisements where for the recovery of data. Unlike the previous search engines, Ask.com returned six of the ten results as relating to the erasure of data, the first of these results being at number 4 on the page.

Combined Results

The search engines returned similar content, considering that the 2011 YouTube video is consistently within the top two results across all platforms.

Table 2- Common Search Engine Results for Data Erasure

Result Title	**Position in Results List**			
	Google	**Bing**	**Yahoo**	**Ask**
How to Erase/Delete All Data from Flash drive Tutorial	1	2	1	1
How to erase all content on USB Flashdrive	2	7		2
Deleting files in your flash drive or memory card using a PC	3	1	3	3
how to clear data from a USB stick on a Mac	4		2	
How to Completely Erase a Memory Stick	5		4	4
How to Delete the Files on a USB Flash Drive	6	5	6	6
Permanently delete files from a flash drive	7		9	8
USB - How do I format my USB Flash Drive on a Mac?	8		8	
data leakage - How do I securely erase USB flash drives	9			10
How do I erase or wipe an old Flash Drive?	10	10	7	7
How can I securely erase files from a USB drive		9		9
How to Delete Everything on a USB Flash Drive			5	5

A large number of search results appear on at least two of the search engines (Table 2). The array of titles suggests information about erasure of data, but unsuspecting users are supplied conflicting information. For example, "How to Erase/Delete All Data from Flash drive Tutorial" is misleading, as the content is about how to format a flash drive and this result is returned as the top option across all platforms. Of concern is that it was posted in 2011 and this poses the question around how and why search engines return particular results.

DISCUSSION

The world as we know it is in the grip of cybercrime epidemic, in 2015 Steve Morgan, writing for Forbes, stated "Cyber-attacks are costing businesses $400 - $500 billion per year" (Morgan, 2015). In 2016 ABC News reported that Cybercriminals are increasingly targeting Australian consumers (Taha, 2016). The threat of identity theft is real, and this research indicates that people, corporations and governments are taking minimal or no precautions to protect their most valuable asset – their sensitive and identifying data. The research projects analysed shows instances of recovering data that could result in the theft of an identity. The result also showed that while the amount of sensitive corporate data recovered is decreasing, it is still being recovered. Consumers are constantly told how an organisation was hacked or succumbed to an attack, and the incidents of identity theft through the theft of hardcopy mail (Edwards, 2015). But there seems to be very little heard on the discovery of information that can be of value to the identity thief through the recovery of remnant data.

The Australian Signals Directorate has posted information on how to protect data from being divulged (ASD, 2016b), but this document and the subsequent information is difficult to locate. In the 2013 Australian research project it was reported that eBay no longer provide warnings to sellers on the sanitisation of data from storage devices put up for sale (Szewczyk, Robins, & Sansurooah, 2013). These warnings where reported as being provided by eBay in the 2011 Australian paper (Szewczyk & Sansurooah, 2011). This may indicate a complacency exhibited in the attitudes of the sellers. Indeed, some private organisations have conducted their own research into remnant data. Avast antivirus company detailed the purchase of 20 used smartphones from eBay and the personal data that was recovered from these devices (Hořejší, 2014). Corporate and government cloud users have the ability and resources to negotiate the level of control they have over not only the sovereignty of their data, but also the level of oversight on the sanitisation of storage media. The average user does not have such an ability, without paying a significant fee.

CONCLUSION

Unless there is a serious effort to increase the level the education, the issue of recoverable remnant data will continue. As the world moves in the direction of a paperless office, the information that will become available increases exponentially. Many households receive utility bills, bank statements and share dividend statements via email. The world's data holdings stood at 4.4 zettabytes in 2013 and is predicted to grow to 44 zettabytes by 2020 (Khoso, 2016). This large quantity of data has the potential to encompass a significant portion of personal and confidential data that could also end up on the second hand market. This paper has highlighted areas that require further research, these being; an in-depth study of how search engines interpret the needs of the user and then display relevant links; and the quality of literature and supporting information that is supplied to end-users in the public domain.

REFERENCES

Adam, A., & Clarke, N. L. (2014). Information Security Leakage: A Forensic Analysis of USB Storage Disks United Kingdom.

Anthoct104 (Writer). (2011). *How to erase all content on USB Flashdrive*. Retrieved from https://www.youtube.com/watch?v=8sDJ0N1uOuw.

ASD. (2016a). *Cloud Computing Security Considerations. Information Security Advice*. Retrieved from http://www.asd.gov.au/publications/protect/cloud_computing_security_considerations.htm

ASD. (2016b). *Data Spill Sanitisation Guide. Canberra Australia: Department of Defence*. Retrieved from http://www.asd.gov.au/publications/protect/data_spill_sanitisation_guide.htm.

Bez, R., & Pirovano, A. (2014). *Overview of non-volatile memory technology: markets, technologies and trends*. In Y. Nishi (Ed.), Advances in Non-volatile Memory and Storage Technology.

eBay. (2016). *eBay*. Retrieved from http://www.ebay.com.au/

eBiz. (2016). *Top 15 Most Popular Search Engines | September 2016*. Retrieved from http://www.ebizmba.com/articles/search-engines

ECU. (2016). *Australian Digital Forensics Conference*. Retrieved from http://ro.ecu.edu.au/adf/index.2.html

Edwards, M. (2015). *Identity theft: More than 770,000 Australians victims in past year*. ABC News. Retrieved from http://www.abc.net.au/news/2015-04-14/identity-theft-hits-australians-veda/6390570

Emam, K. E., Neri, E., & Jonker, E. (2007). An Evaluation of Personal Health Information Remnants in Second-Hand Personal Computer Disk Drives. *JMIR Publications*, 9(3).

Farden, M. A., & Diesburg, S. (2014). *Analysis Of Deletion Habits On Used USB Thumb Drives*. In U. o. N. Iowa (Ed.).

Fragkos, G., Mee, V., Xynos, K., & Angelopoulou, O. (2006). *An empirical methodology derived from the analysis of information remaining on second hand hard disks.* Paper presented at the Second European Conference on Computer Network Defence.

Gutmann, P. (1996). *Secure Deletion of Data from Magnetic and Solid-State Memory*. Auckland, New Zealand.

Hořejší, J. (2014, 9 July 2014). *How Avast recovered 'erased' data from used Android phones*. Retrieved from https://blog.avast.com/2014/07/09/android-foreniscs-pt-2-how-we-recovered-erased-data/

Jones, A., MArtin, T., & Alzaabi, M. (2012). *The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE*. Paper presented at the 10th Australian Digital Forensics Conference, Perth Western Australia.

Jones, A., Valli, C., & Dabibi, G. (2009). *The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market*. Paper presented at the 7th Australian Digital Forensic Conference, Perth Western Australia.

Jones, A., Valli, C., Dardick, G. S., Sutherland, I., & Dabibi, G. (2009). *The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market*. Paper presented at the 8th Australian Digital Forensics Conference, Perth Western Australia.

Khoso, M. (2016, 13 May 2016). *How Much Data is Produced Every Day?* Retrieved from http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/

Li, J. (2016). *Worldwide Personal & Entry-Level Storage Market Declined in 2015*, According to IDC International Data Corporation, IDC tracker. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS41021816

Mee, V. (2008). Who is Reading the Data on Your Old Computer? *Journal of Digital Forensics, Security and Law*, 3(1), 25-34.

Morgan, S. (2015). *The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics*. Retrieved from http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#130eeabe10b2

OAIC. (2013). *Australian Privacy Principles*. Retrieved from https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

ReportBuyer. (2015). *Global Digital Storage Devices Market Outlook (2014-2022).* PR Newswire. Retrieved from http://www.prnewswire.com/news-releases/global-digital-storage-devices-market-outlook-2014-2022-300145285.html

Rivera, L. (Writer). (2011). *How to Erase/Delete All Data from Flash drive Tutorial --(Even hidden files!).* Retrieved from https://www.youtube.com/watch?v=8wWB6Ee469I

Roberts, D., & Wolfe, H. B. (2011). *Data remanence in New Zealand: 2011*. Paper presented at the 9th Australian Digital Forensics Conference, Perth, Western Australia.

Robins, N., Williams, P. A. H., & Sansurooah, K. (2015). *I know what you did last summer… An Investigation into Remnant Data on USB Storage Devices Sold in Australia in 2015*. Paper presented at the Australasian Computer Science Week, Canberra Australia.

SanDisk. (2008). *Deleting files in your flash drive or memory card using a PC*. Retrieved from http://kb.sandisk.com/app/answers/detail/a_id/2281/~/deleting-files-in-your-flash-drive-or-memory-card-using-a-pc

Shah, A. (2016). *Samsung's massive 32TB SSD includes cutting-edge 3D chip technology*. Retrieved from http://www.pcworld.com/article/3105875/storage/samsungs-massive-32tb-ssd-includes-cutting-edge-3d-chip-technology.html.

Sliwa, C. (2016). *Flash technologies remain hot in 2016, experts predict*. Retrieved from http://searchsolidstatestorage.techtarget.com/news/4500273061/Flash-technologies-remain-hot-in-2016-expects-predict.

Szewczyk, P., Robins, N., & Sansurooah, K. (2013a). *Sellers Continue to Give Away Confidential Information on Second Hand Memory Cards Sold in Australia*. Paper presented at the 11th Australian Digital Forensics Conference, Perth, Western Australia.

Szewczyk, P., & Sansurooah, K. (2011). *A 2011 investigation into remnant data on second hand memory cards sold in Australia*. Paper presented at the 9th Australian Digital Forensics Conference, Perth, Western Australia.

Szewczyk, P., & Sansurooah, K. (2012). *The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia*. Paper presented at the 10th Australian Digital Forensic Conference, Perth, Western Australia

Taha, M. (2016). *Cybercriminals increasingly targeting Australia as a launch pad for cybercrime*. ABC News. Retrieved from http://www.abc.net.au/news/2016-02-26/cyber-criminals-increasingly-targeting-australia/7203478

Valli, C., & Woodward, A. (2007). *Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks*. Paper presented at the 5th Australian Digital Forensics Conference, Perth, Western Australia.

Valli, C., & Woodward, A. (2008). *The 2008 Australian study of remnant data contained on 2nd hand hard disks: the saga continues*. Paper presented at the 6th Australian Digital Forensics Conference, Perth, Western Australia.